PCT/JP2004/003533

日本国特許庁
JAPAN PATENT OFFICE

23.04.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月１７日

出願番号
Application Number: 特願２００３－０７２３７２

[ST. 10/C]: [ＪＰ２００３－０７２３７２]

出願人
Applicant(s): セイコーエプソン株式会社

２００４年　６月　２日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０４７１２８

【書類名】　特許願
【整理番号】　J0096564
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/00
【発明者】
　【住所又は居所】　長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
　【氏名】　黒田　直人
【特許出願人】
　【識別番号】　000002369
　【氏名又は名称】　セイコーエプソン株式会社
【代理人】
　【識別番号】　100095728
　【弁理士】
　【氏名又は名称】　上柳　雅誉
　【連絡先】　０２６６－５２－３１３９
【選任した代理人】
　【識別番号】　100107076
　【弁理士】
　【氏名又は名称】　藤綱　英吉
【選任した代理人】
　【識別番号】　100107261
　【弁理士】
　【氏名又は名称】　須澤　修
【手数料の表示】
　【予納台帳番号】　013044
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0109826

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラム

【特許請求の範囲】

【請求項１】　ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項２】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項３】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、

当該プログラムの起動時の、ネット接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項４】　コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する、制御プログラムを、

自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項５】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【請求項６】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【請求項７】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項８】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムによる、ネット接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項９】　請求項１に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【請求項１０】　ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

【請求項１１】　コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

前記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ウィルス対策ソフトによる定義ファイルの修正分取り込み処理等の制御により、ネットワーク接続時のセキュリティを高めたネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラムに関する。

【０００２】

【従来の技術】

コンピュータウィルスに対する対策のためにコンピュータにインストールされた対策ソフトは、通常、コンピュータを起動したときに立ち上がる。そして、コンピュータをネットワークに接続すると、一定時間おきにネットワークを通じて所定のサーバに接続し、ウィルス対策用定義ファイルの定義ファイルの修正分取り込み処理をする。即ち、定義ファイルのバージョンが変わっている場合には、差分を取り込んだり、更新されたファイル全体を取り込むことにより、定義ファイルを更新する。その後は、同様の処理を自動的に周期的に繰り返す。こうしたワクチンやパターンファイルの更新技術が紹介されている（特許文献１参照）。

【特許文献１】　特開２００２－２５９１５０号公報

【０００３】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

モバイルコンピュータは、ネットワークに接続される前に起動して、ローカルで使用されることが多い。ウィルス対策ソフトはモバイルコンピュータの起動と同時に起動して、周期的に定義ファイルの修正分取り込み処理を試みるが、ネットワークに接続されていないから、ファイルの更新に失敗する。場合によっては

、長期間定義ファイルの修正分取り込み処理がなされないままになっていることもある。こうしたコンピュータを起動させたままの状態で、突然ネットワークに接続すると、ウィルス対策ソフトが次のタイミングで定義ファイルの修正分取り込み処理を実行するまでは、新種のウィルスに対し、無防備な状態になる。

本発明は、以上の点に着目してなされたもので、通信を実行するプログラムの起動時に、自動的にセキュリティ対策用ファイルの更新処理を実行させるようにしたネットワークセキュリティ強化システムとネットワークセキュリティ強化プログラムを提供することを目的とする。

【０００４】

【課題を解決するための手段】

本発明は次の構成により上記の課題を解決する。

〈構成１〉

ネットワークに接続をして通信を実行するプログラムの起動時に、上記ネットワークへの接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【０００５】

セキュリティ対策用ファイルの更新処理とは、ウィルス対策用の定義ファイルの修正分取り込み処理や、パッチファイルの取り込み処理のように、コンピュータをネットワークに接続した場合のセキュリティ対策用ファイルを、ネットワークを通じて取得して更新する処理のことである。修正分は、差分データのこともあるし、修正して更新されたデータファイルのこともある。この処理は、ネットワークに接続をして通信を実行するプログラムの起動時に実行される。ネット接続処理後他の処理に先行するから、通信を実行するプログラムの動作開始前に最新のセキュリティ対策が施される。ネットワークへの接続が長時間に及ぶ場合は、その後一定時間おきにセキュリティ対策用ファイルの更新処理を起動することが好ましい。

【０００６】

〈構成２〉

構成１に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【０００７】

セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力することで、利用者は、安心してネットワークを利用できる。また、動作エラーにより無防備な状態になったときは、ネットワークを切断する等の処置ができる。

【０００８】

〈構成３〉

構成１に記載のネットワークセキュリティ強化システムにおいて、既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、当該プログラムの起動時の、ネット接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【０００９】

ネットワーク接続後はウィルス対策プログラムが定期的に動作するから、その後通信を実行するプログラムの再立ち上げや追加立ち上げをしても、セキュリティ対策用ファイルの更新処理をさせない。これにより、通信を実行するプログラムの立ち上げ処理が速くなる。

【００１０】

〈構成４〉

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する、制御プログラムを、自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【００１１】

上記の構成のシステムを実現するには、ネット接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動するという制御プログラムが必要である。しかしながら、コンピュータによって、インストールされている通信用のプログラムが異なる。そこで、あらかじめ、コンピュータにインストールされた、通信用のプログラムを検出し、自動的に制御プログラムを生成する手段を設けた。これにより、各種の通信用プログラムをインストールした任意のコンピュータに対して、上記の機能を容易に付与できる。

【００１２】

〈構成５〉

構成１に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【００１３】

セキュリティ対策として最も重要な処理である。

【００１４】

〈構成６〉

構成１に記載のネットワークセキュリティ強化システムにおいて、セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

【００１５】

セキュリティホール対策として、パッチファイルの取り込みを先行させることも重要である。

【００１６】

〈構成７〉

構成１に記載のネットワークセキュリティ強化システムにおいて、ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【００１７】

ブラウザを立ち上げる場合には、始めに定義ファイルの修正分取り込み処理を行い、その後ブラウザの画面表示を実行する。ブラウザの画面表示をしたときには、既にネットワークからウィルスが侵入するおそれがあるからである。

【００１８】

〈構成８〉

構成１に記載のネットワークセキュリティ強化システムにおいて、ネットワークに接続をして通信を実行するプログラムによる、ネット接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【００１９】

メールソフトやブラウザやダイヤルアッププログラムなどの立ち上げ時の画面に、定義ファイルの更新をして下さい、というメッセージが表示出力される。メッセージは音声で出力されても構わない。セキュリティ対策用ファイルの更新処理は、通信を実行するプログラムと連動していなくて構わない。この場合には、無用なファイル更新処理を回避することができる。

【００２０】

〈構成９〉

構成１に記載のネットワークセキュリティ強化システムにおいて、ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

【００２１】

ブラウザの起動時に、定義ファイルやパッチファイルの更新をして下さい、というメッセージが表示出力される。従って、自動化はされないが、セキュリティは確保される。

【００２２】

〈構成１０〉

ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

【００２３】

構成１のシステムを実現するためのコンピュータプログラムの発明である。

【００２４】

〈構成１１〉

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、上記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。

【００２５】

構成４の制御プログラムを自動的に生成するプログラムの発明である。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態を、具体例を用いて説明する。

図１は、ネットワークセキュリティ強化システムの具体例を示すブロック図である。

図のように、セキュリティ強化の対象になっているコンピュータ１０は、ネットワークインタフェース１１を介してネットワーク１に接続されている。コンピュータ１０には、記憶装置１２と演算処理装置が設けられている。演算処理装置は、メーラー（メール管理プログラム）１３とブラウザ１４とダイヤルアッププログラム１５とウィルス対策プログラム１６とネット接続制御プログラム１７から構成される。ウィルス対策プログラム１６は、定義ファイル修正分取り込みプログラム１８を備える。これらの演算処理装置は、コンピュータ１０を動作させるコンピュータプログラムからなる。ネットワーク１にはウィルス対策プログラムの提供元のサーバ２０が接続されている。このサーバ２０には記憶装置２１が

設けられており、定義ファイル２２を、ネットワーク１を通じてユーザに提供するようにしている。

【００２７】

メーラー（メール管理プログラム）１３は、メールの送受信を制御するプログラムである。ブラウザ１４は、インターネット閲覧用のプログラムである。ダイヤルアッププログラム１５は、あらかじめ設定された電話番号に対してダイヤルアップ接続をする制御を行うプログラムである。ウィルス対策プログラム１６は、ウィルスチェックを実行するプログラムである。ウィルス対策プログラム１６が動作するためには定義ファイル２２が必要になる。ウィルス対策プログラム１６の提供元は、新たなウィルスが発生するたびに定義ファイル２２の修正分ファイルを提供する。ウィルス対策プログラム１６は、あらかじめ設定された時間間隔で周期的に定義ファイル修正分取り込みプログラム１８を起動する。定義ファイル修正分取り込みプログラム１８は、所定のタイミングで定期的にサーバ２０から定義ファイル２２をダウンロードし記憶装置１２に記憶させる機能を持つ。

【００２８】

ネット接続制御プログラム１７は、メーラー（メール管理プログラム）１３やブラウザ１４を利用するために、ユーザがいずれかを起動すると、まず、ダイヤルアッププログラム１５を起動し、次にウィルス対策プログラム１６の定義ファイル修正分取り込みプログラム１８を起動する。こうして、通信用のプログラムを実行する前に、まず、定義ファイル２２を最新のものに更新しておく機能を持つ。この発明では、メールソフトやブラウザやダイヤルアッププログラムなど、ネットワークに接続をして通信を実行するプログラムの起動時に、自動的にウィルス対策ソフトによる定義ファイルの修正分取り込み処理を実行させる。これによって、常に最新の定義ファイルを利用し、例えば、モバイルコンピュータがネットワークを通じて安全に通信をすることができる。

【００２９】

図２は、ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。

この図を、図１と比較して説明する。コンピュータ１０には、ウィルス対策プ

ログラム１６の代りにパッチファイル取り込みプログラム１９が設けられている。なお、１台のコンピュータにウィルス対策プログラム１６とパッチファイル取り込みプログラム１９を合わせて備えることが好ましいが、説明の都合上それぞれ独立に実例を示した。ネット接続制御プログラム１７は、ダイヤルアッププログラム１５を起動した後に、パッチファイル取り込みプログラム１９を起動するように動作する。ネットワーク１にはサーバ２５が接続されている。このサーバ２５は、メーラー（メール管理プログラム）１３やブラウザ１４を提供する提供元が管理する。サーバ２５に設けられた記憶装置２６には、メーラー（メール管理プログラム）１３やブラウザ１４のセキュリティ改善のためのパッチファイル２３が記憶されている。パッチファイル取り込みプログラム１９は、ネットワーク１を通じてパッチファイル２３をダウンロードし記憶装置１２に記憶する機能を持つ。このパッチファイル２３によってメーラー（メール管理プログラム）１３やブラウザ１４がその都度更新される。

【００３０】

図３は、図１に示したプログラムの動作中表示される画面例の説明図である。

既に説明したように、例えば、メーラーの起動がされると、ダイヤルアッププログラム１５の処理が開始されて、ネットワークの接続条件の設定が行われる。続いて、ウィルス対策プログラム１６の定義ファイル修正分取り込みプログラム１８が起動して、自動的に定義ファイルの修正分取り込み処理が実行される。このとき、その処理が完了したことをユーザに伝えるために、図３（ａ）の画面３１が表示される。ここでは、ユーザに対し、「ウィルス定義ファイルの更新をしました」というメッセージを表示し、その後安心してメーラー（メール管理プログラム）１３を利用できることをユーザに伝える。ユーザは、ボタン４１をクリックしてこの画面３１を閉じる。その後はメーラー（メール管理プログラム）１３が起動して通常通りメールの送受信が可能になる。なお、ブラウザは画面を表示すると既にネットワークを通じて初期画面のダウンロードを開始する。従って、ブラウザの画面表示より前に、定義ファイル２２の更新処理やブラウザのパッチファイルを当てる処理を実行しておくことが好ましい。

【００３１】

ウィルス定義ファイルの修正分取り込み処理は、既知の方法でよく、例えば、ＸＭＬデータベース形式でサーバからダウンロードして、アップデートすればよい。また、アプリケーションプログラムのセキュリティホール修復の目的で、アプリケーションプログラム供給元から配布される。パッチファイル２３の取得とパッチを当てる処理についても、同様の手順で実行できる。図３（ｂ）は後者の場合の、表示画面３２の例である。また、定義ファイル２２やパッチファイル２３の更新処理を実行する前に、ユーザの了解をとる方法もある。この場合には、図３（ｃ）に示す画面３３のように、「インターネット接続前にウィルス定義ファイルの更新をします」といったメッセージを表示する。

【００３２】

ボタン４３をクリックするとユーザの了解が得られた状態になり、定義ファイル更新分取り込みプログラム１８が起動する。パッチファイル取り込みプログラム１９の起動についても同様の制御が可能である。このほかに、定義ファイル２２やパッチファイル２３の更新処理をユーザの制御により実行することもできる。図３の（ｄ）に示す画面３４のように、ネットワークの接続条件設定直後に、「メール送受信の開始前にセキュリティ対策ファイルの更新をして下さい」といったメッセージを表示する。この画面で、ボタン４４をクリックすると定義ファイル２２の更新処理が実行される。またボタン４５をクリックするとパッチファイル２３の更新処理が実行される。

【００３３】

図４は、ネット接続制御プログラム１７をインストールしたときの動作説明図である。

ネット接続制御プログラム１７は、多数のコンピュータにインストールされて、その機種を選ばず動作するように、以下の機能を持つことが好ましい。図４（ａ）の画面３５に示すように、初めに、インストールされるべきコンピュータの通信用ソフトを検索する。そして、制御対象になるソフトを決定する。画面３５には、リストボックス３７とボタン４６～５０が設けられている。インストール直後、リストボックス３７にコンピュータ中の通信用ソフトのリストを表示する。ユーザがこの中から普段使用しているメーラーとブラウザを選択する。不要な

ものはボタン４８をクリックして削除する。また、ほかにも通信用ソフトがある場合には、ボタン４６を押して追加する。リストに表示させるにはボタン４７をクリックすればよい。こうして、制御の対象となる通信用ソフトを決定すると、ボタン４９をクリックする。ボタン５０ですべての処理をキャンセルすることもできる。以上の準備処理によって図４の（ｂ）に示すような起動画面を生成する。

【００３４】

起動画面３８は、上記のようなネットワークセキュリティの強化を図りながら、メールやインターネットを利用するための、新たなアプリケーションの画面である。この画面３８には、例えば「ネットワーク接続ユーティリティ」といった表題が付けられている。ボタン５１をクリックするとメーラーが起動する。ボタン５２をクリックするとブラウザが起動する。制御プログラムは、図のような画面３８を表示するフォームと、ボタン５１と５２のクリックイベントにより実行されるコマンドのリストが含まれる。そのコマンドの意味は、画面３８の下側に示したとおりである。

【００３５】

図５は、ネット接続制御プログラムの動作フローチャートである。

図５（ａ）は、ネット接続制御プログラム１７の具体的な動作フローチャートである。まず、ステップＳ１で、通信用プログラムの起動指示を待つ。図４の（ｂ）に示した画面３８を使用して、ボタン５１をクリックしメーラーを起動した場合には、ステップＳ１からステップＳ２へ進む。ステップＳ２では、制御シーケンスを起動する。制御シーケンスとは、ステップＳ３からステップＳ７の、一連の処理のことである。ステップＳ３で、ダイヤルアップ接続を起動する。そして、ステップＳ４で接続を確立させる。これでネットワークとの接続が可能になったから、ステップＳ５で、修正分取り込み処理を起動させて、定義ファイル２２の修正分をダウンロードさせる。もちろん、同時に、パッチファイル２３のダウンロードを実行させることもできる。その後、ステップＳ６で、処理完了メッセージを表示する。最後に、ステップＳ７で、通信用プログラムを起動して処理を終了する。

【００３６】

図５（ｂ）は、制御プログラムのオプションとして設けられたプログラムである。ネットワークに接続をして既に定義ファイル２２やパッチファイル２３の更新処理を済ませた後、いったん通信用プログラムも終了させることがある。この場合に、ネットワークの接続を継続していれば、定義ファイル修正分取り込みプログラム１８やパッチファイル取り込みプログラム１９はそのまま正常に動作している。従って、一定時間おきに定義ファイル２２やパッチファイル２３の更新処理が自動的に実行されている。その後再び通信用プログラムを起動したときに、改めて起動時に定義ファイル２２やパッチファイル２３の更新処理を実行する必要はない。さもなければ、通信用プログラムの起動に時間がかかり操作性を悪くする。そこで、図のステップＳ２１で、ネットワーク接続中かどうかを判断する。ネットワークに接続中であれば、ステップＳ２２で、接続後に更新したかどうかを判断する。接続後に１回でも更新をした履歴が記録されていれば、ステップＳ２３で、制御プログラムの起動を中止する。もちろん、いったんネットワークを切断してしまった場合には、制御プログラムを起動させる。

【００３７】

図６は、ネット接続制御プログラムの別の動作フローチャートである。

図６（ａ）は、ネット接続制御プログラム１７をインストールしたときの初期設定動作を示すフローチャートである。まず、ステップＳ３１で、インストールを完了すると、ステップＳ３２で、通信用プログラムの検索をする。そして、ステップＳ３３で、通信用プログラムリストを生成する。ここで、その結果を表示し、ステップＳ３４で、追加要求があれば、ステップＳ３５でリストに対し通信用プログラムの追加処理を実行する。ステップＳ３６で、削除要求あれば、ステップＳ３７でリストの一部を削除処理する。最後に、ステップＳ３８で、制御プログラムの生成をする。図６（ｂ）は、ネット接続制御プログラム１７の起動制御をユーザに任せる場合のプログラムフローチャートである。即ち、ステップＳ４１で、通信用プログラムの起動指示があると、ステップＳ４２で、制御プログラムの起動を要求する画面を表示する。いずれかのボタンがクリックされると、該当するプログラムが起動する。この処理は既に説明をしたとおりである。

【００３８】

上記のようにして、ネットワークに接続をして通信を実行するプログラムの起動時に、ネット接続処理後他の処理に先行して、必ず、セキュリティ対策用ファイルの更新処理を起動させるようにしたので、例えば、長期間定義ファイルの更新をしないまま使用していたコンピュータを突然ネットワークに接続した場合でも、ウィルスの侵入から確実にコンピュータを防御できる。

【００３９】

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウエアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

【図面の簡単な説明】

【図１】　ネットワークセキュリティ強化システムの具体例を示すブロック図である。

【図２】　ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。

【図３】　図１に示したプログラムの動作中表示される画面例の説明図である。

【図４】　ネット接続制御プログラムをインストールしたときの動作説明図である。

【図５】　ネット接続制御プログラムの動作フローチャートである。

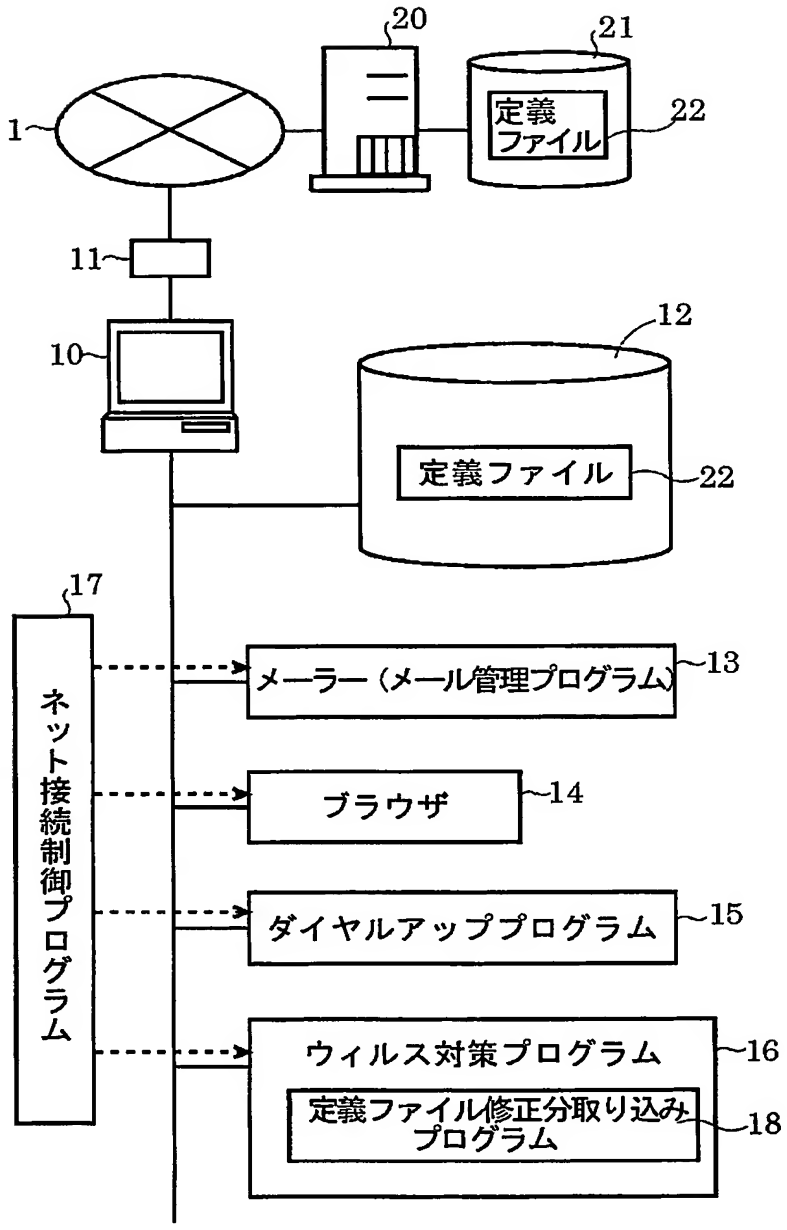
【図６】　ネット接続制御プログラムの別の動作フローチャートである。

【符号の説明】

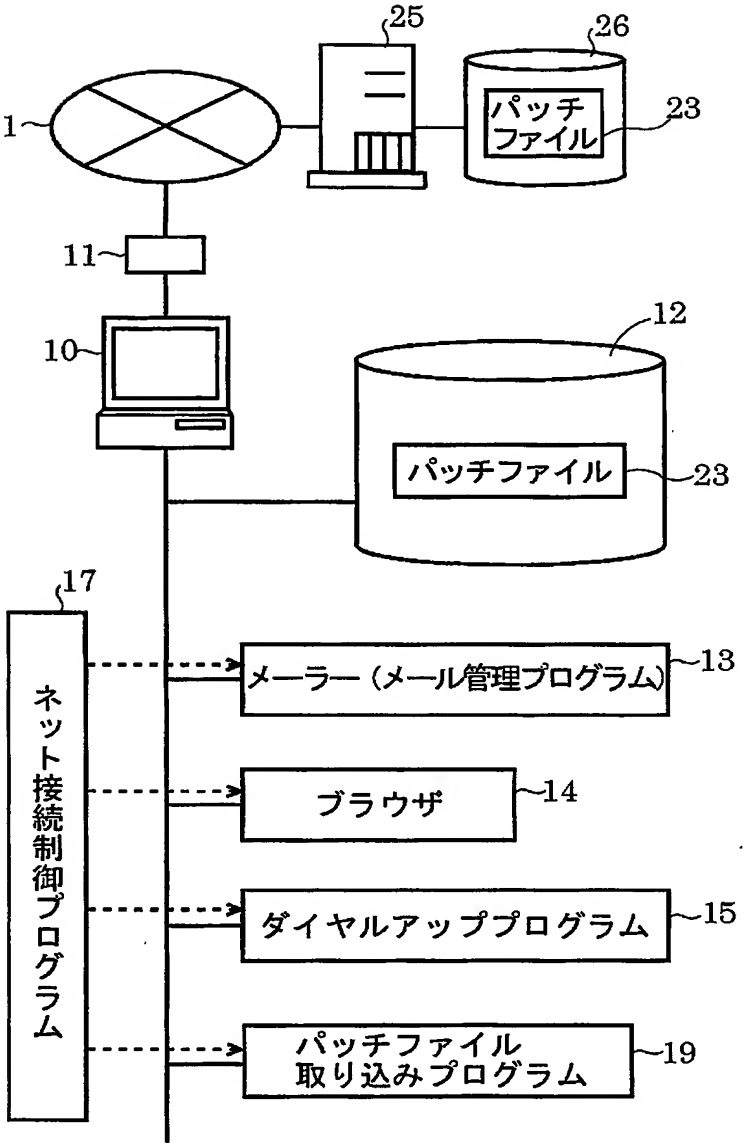
１　ネットワーク、　１０　コンピュータ、　１１　ネットワークインタフェース、　１２　記憶装置、　１３　メーラー（メール管理プログラム）、　１４　ブラウザ、　１５　ダイヤルアッププログラム、　１６　ウィルス対策プログラム、　１７　ネット接続制御プログラム、　１８　定義ファイル修正分取り込みプログラム、　１９　パッチファイル取り込みプログラム、　２０　サーバ、　２１　記憶装置、　２２　定義ファイル

【書類名】図面

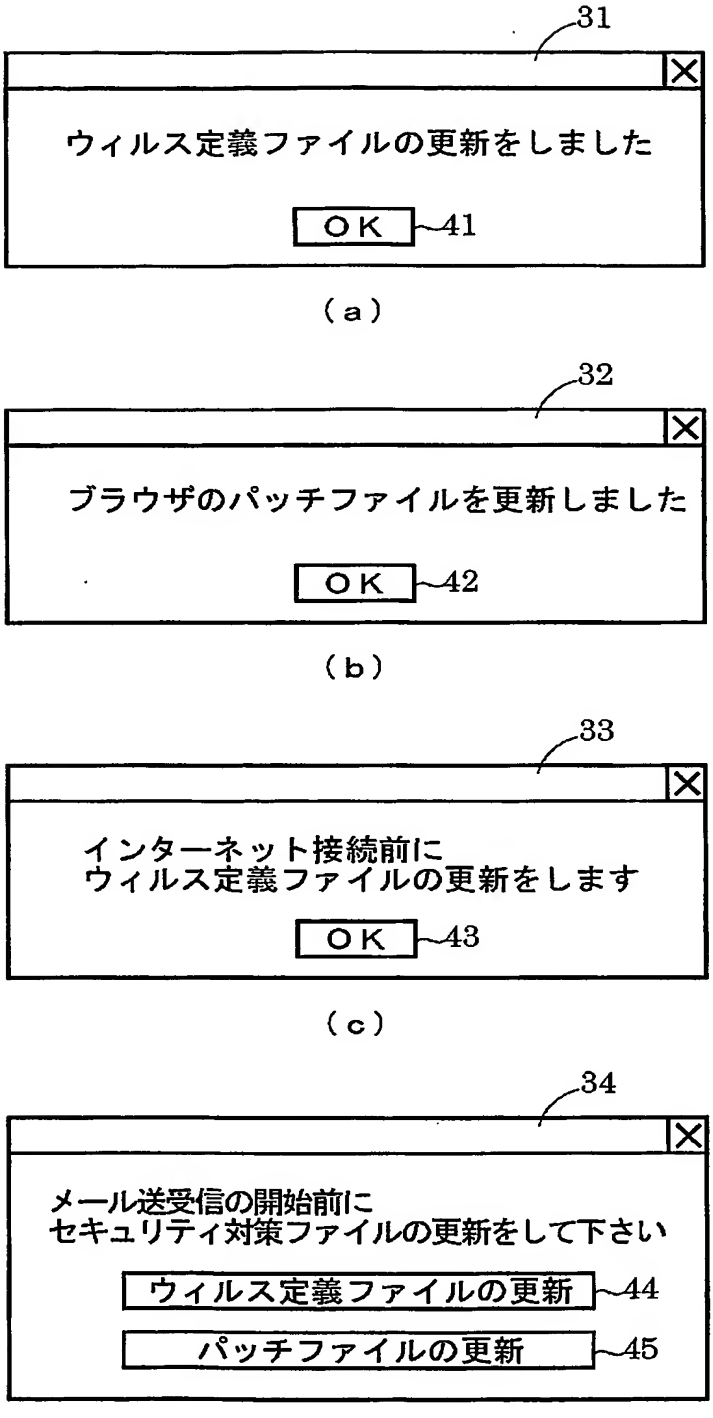
【図１】


20
21
1
定義
ファイル
22
11
12
10
定義ファイル
22
17
ネット接続制御プログラム
メーラー（メール管理プログラム）
13
ブラウザ
14
ダイヤルアッププログラム
15
ウィルス対策プログラム
16
定義ファイル修正分取り込み
プログラム
18

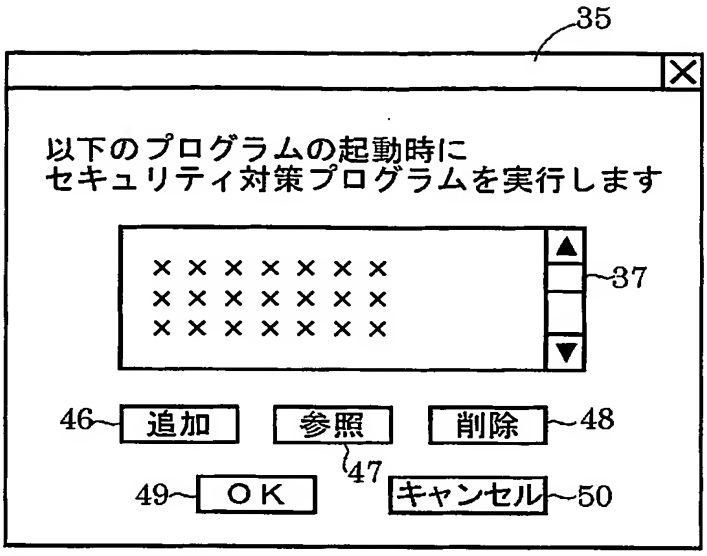
【図２】


25
26
1
パッチ
ファイル
23
11
12
10
パッチファイル
23
17
ネット接続制御プログラム
メーラー（メール管理プログラム）
13
ブラウザ
14
ダイヤルアッププログラム
15
パッチファイル
取り込みプログラム
19

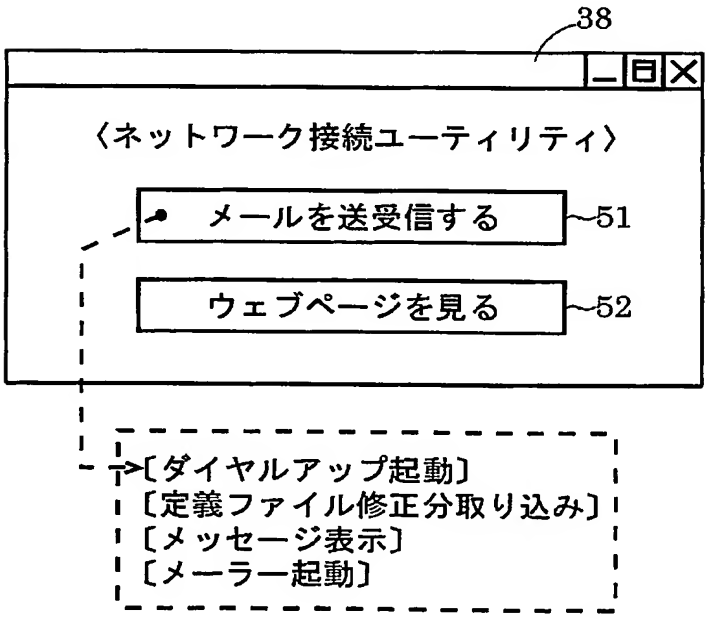
【図３】


31
ウィルス定義ファイルの更新をしました
OK
41
(a)
32
ブラウザのパッチファイルを更新しました
OK
42
(b)
33
インターネット接続前に
ウィルス定義ファイルの更新をします
OK
43
(c)
34
メール送受信の開始前に
セキュリティ対策ファイルの更新をして下さい
ウィルス定義ファイルの更新
44
パッチファイルの更新
45
(d)

【図４】


35
以下のプログラムの起動時に
セキュリティ対策プログラムを実行します
×××××××
×××××××
×××××××
37
46
追加
参照
削除
48
47
49
ＯＫ
キャンセル
50

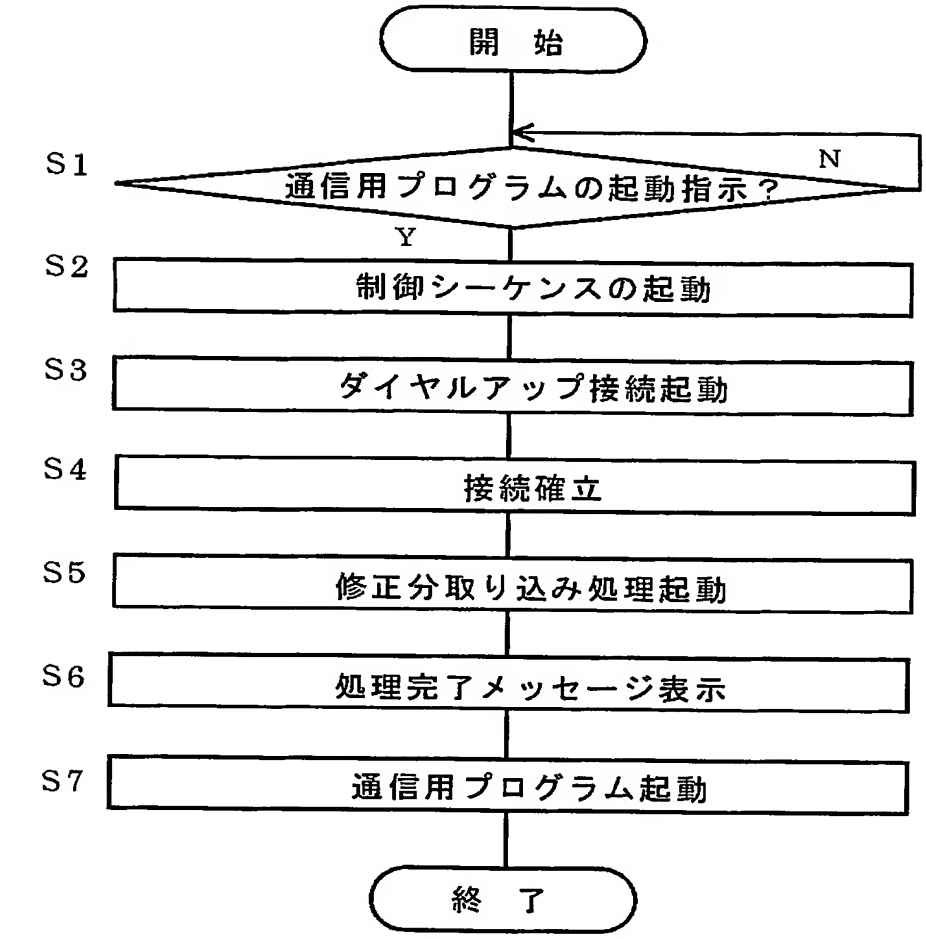
（ａ）


38
〈ネットワーク接続ユーティリティ〉
メールを送受信する
51
ウェブページを見る
52
〔ダイヤルアップ起動〕
〔定義ファイル修正分取り込み〕
〔メッセージ表示〕
〔メーラー起動〕

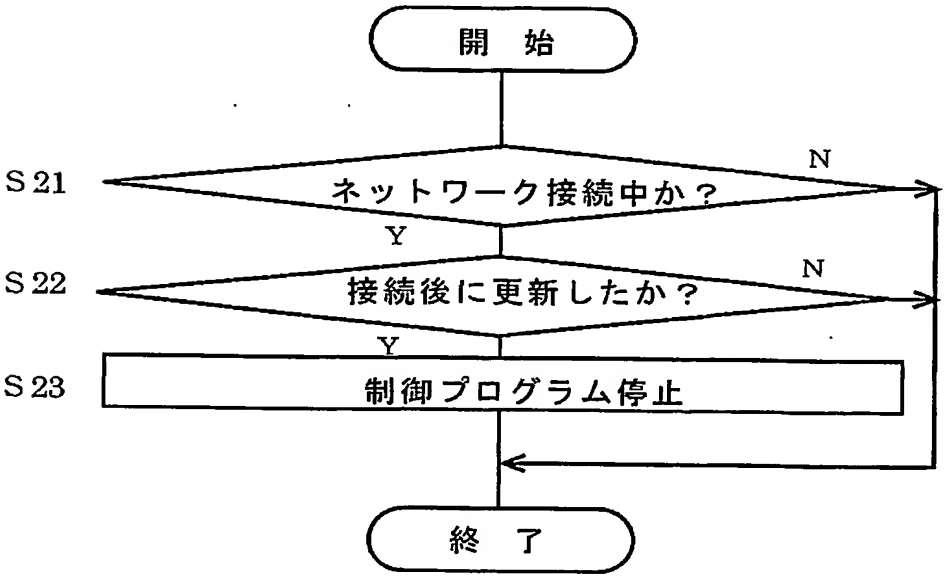
（ｂ）

【図５】

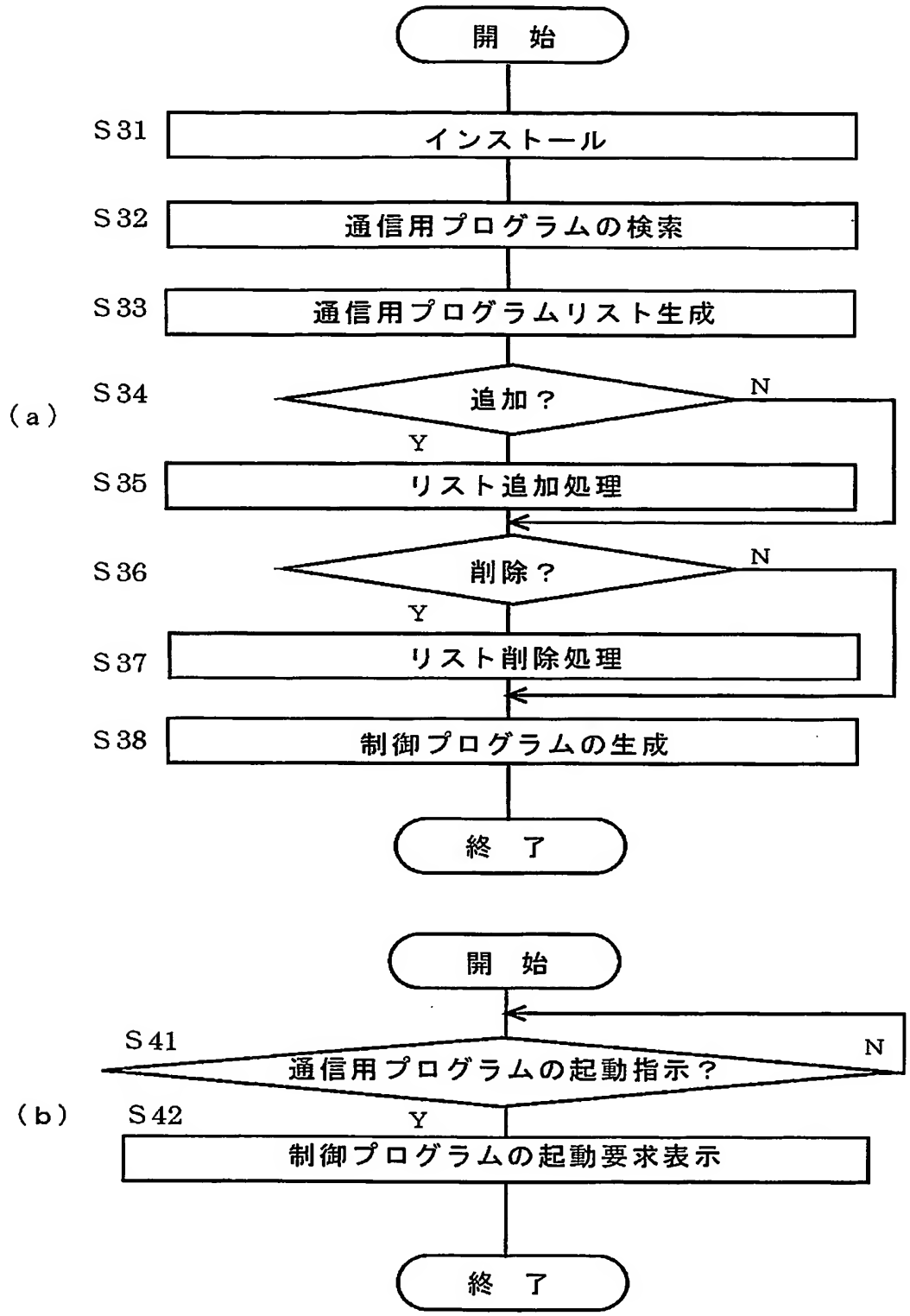
（ａ）


開　始
S1
通信用プログラムの起動指示？
N
Y
S2
制御シーケンスの起動
S3
ダイヤルアップ接続起動
S4
接続確立
S5
修正分取り込み処理起動
S6
処処理完了メッセージ表示
S7
通信用プログラム起動
終　了

（ｂ）


開　始
S21
ネットワーク接続中か？
N
Y
S22
接続後に更新したか？
N
Y
S23
制御プログラム停止
終　了

【図６】


開　始
S31
インストール
S32
通信用プログラムの検索
S33
通信用プログラムリスト生成
S34
追加？
N
Y
S35
リスト追加処理
S36
削除？
N
Y
S37
リスト削除処理
S38
制御プログラムの生成
終　了
(a)
開　始
S41
通信用プログラムの起動指示？
N
Y
S42
制御プログラムの起動要求表示
終　了
(b)

【書類名】　要約書

【要約】

【課題】　常に最新のウィルス定義ファイルやパッチファイルを利用し、モバイルコンピュータがネットワークを通じて安全に通信ができるようにする。

【解決手段】　メールソフトやブラウザやダイヤルアッププログラムなど、ネットワークに接続をして通信を実行するプログラムの起動時に、自動的にウィルス対策ソフトを起動させる。そして、通信開始前に定義ファイルの修正分取り込み処理やパッチファイル更新処理を実行させる。さらに、セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０７２３７２
受付番号	５０３００４３３９６９
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月１８日

＜認定情報・付加情報＞

【提出日】　平成15年 3月17日

次頁無

特願２００３－０７２３７２

出　願　人　履　歴　情　報

識別番号　［０００００２３６９］

１．変更年月日　１９９０年　８月２０日
［変更理由］　新規登録
住　所　東京都新宿区西新宿２丁目４番１号
氏　名　セイコーエプソン株式会社